

# System Strategies References

---

Bob Ellison, CERT, Software Engineering Institute [vita<sup>1</sup>]  
Carol Woody, CERT, Software Engineering Institute [vita]

Copyright © 2007 Carnegie Mellon University

2007-05-17

System Strategies bibliography.

## References

- [Berg 06] Berg, Clifford J. *High Assurance Design: Architecting Secure and Reliable Enterprise Applications*. Upper Saddle River, NJ: Addison-Wesley, 2006.
- [Boehm 04] Boehm, Barry & Turner, Richard. *Balancing Agility and Discipline: A Guide for the Perplexed*. Boston, MA: Addison-Wesley Professional, 2003 (ISBN 0-321-18612-5).
- [Boehm 06] Boehm, Barry. "Some Future Trends and Implications for Systems and Software Engineering Processes." *Systems Engineering* 9, 1 (Spring 2006): 1-19.
- [Booch 05] Booch, Grady. [Architecture Web Log](#)<sup>3</sup> (2005).
- [Booch 06] Booch, Grady. [The Architecture Handbook](#)<sup>4</sup>. (Registration required.)
- [DoD 99a] U.S. Department of Defense. *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. DoD Instruction 5200.40, November 30, 1999.
- [Kantor 05] Kantor, A. "Kutztown Kids Aren't the Good Guys." *USA Today*, August 18, 2005.
- [Leveson 05] Leveson, Nancy G. "A Systems-Theoretic Approach to Safety in Software-Intensive Systems." *IEEE Transactions on Dependable and Secure Computing* 1, 1 (January-March 2004): 66-86.
- [Lindsay 04] Lindsay, Bruce. "[Engineering for Failure](#)"<sup>5</sup>. *ACM Queue* 2, 8 (November 2004).
- [Maier 06] Maier, Mark W. "System and Software Architecture Reconciliation." *Systems Engineering* 9, 2 (Summer 2006): 146-158.
- [Maier 98] Maier, Mark W. "[Architecting Principles for Systems-of-Systems](#)"<sup>6</sup>. *Systems Engineering* 1, 4 (Winter 1998): 267-284.

---

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/208-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/208-BSI.html) (Ellison, Robert J.)

- [McGraw 06] McGraw, Gary. *Software Security: Building Security In*. Upper Saddle River, NJ: Addison-Wesley Professional, 2006 (ISBN 0-321-35670-5).
- [McIlroy 68] McIlroy, M. D. "Mass Produced Software Components," 138-151. *Software Engineering: Report on a Conference Sponsored by the NATO Science Committee*. Garmisch, Germany, Oct. 7-11, 1968. Brussels, Belgium: Scientific Affairs Division, NATO, 1968.
- [Neumann 00] Neumann, Peter G. "[Practical Architectures for Survivable Systems and Networks](#)<sup>7</sup>." Menlo Park, CA: Computer Science Laboratory, SRI International, June 2000.
- [Neumann 04] Neumann, Peter G. [Principled Assuredly Trustworthy Composable Architectures](#)<sup>8</sup> (Final Report to DARPA, CDRL A001). Menlo Park, CA: Computer Science Laboratory, SRI International, December, 28, 2004.
- [Neumann 06] Neumann, Peter G. "Risks Relating to System Compositions." *Communications of the ACM* 49, 7 (July 2006): 120.
- [Perrow 99] Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. Princeton, NJ: Princeton University Press, 1999 (ISBN 0-691-00412-9).
- [Rechtin 91] Rechtin, E. *System Architecting: Creating and Building Complex Systems*. Englewood Cliffs, NJ: Prentice Hall, 1991.
- [Rushby 02] Rushby, John. *Modular Certification* (CSL Report). Menlo Park, CA: SRI International, 2002.
- [Rushby 83] Rushby, J. M. & Randell, B. "A Distributed Secure System," 127-135. *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, CA, April 25-27, 1983. Maryland: IEEE Computer Society Press, 1983.
- [Russell 05] Russell, J. & Theodore, E. "[Drug Records, Confidential Data Vulnerable](#)<sup>9</sup>." *The Harvard Crimson*, January 21, 2005.
- [Saltzer 75] Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63, 9 (September 1975): 1278-1308.
- [Schneider 99] Schneider, Fred B., ed. [Trust in Cyberspace](#)<sup>10</sup>. Washington, DC: National Academy Press, 1999.
- [SEI 06] Software Engineering Institute. [Ultra-Large-Scale Systems: The Software Challenge of the Future](#)<sup>11</sup> (2006).

[Smith 05]

Smith, S. "Pretending That Systems are Secure." *IEEE Security & Privacy* 3, 6 (November/December 2005): 73-76.

[US-Canada 04]

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*<sup>12</sup>. April 2004.

## Carnegie Mellon Copyright

---

Copyright © Carnegie Mellon University 2005-2010.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

### NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

---

1. <mailto:permission@sei.cmu.edu>